Lecture 5

Recall: $m \in \mathbb{Z}$, $m \geq 1$

$$\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, 3, \ldots, m-1\}$$

↓

Class, not just a number

$\mathbb{Z}/m\mathbb{Z}$ is a group with respect to addition.

Although multiplication is also a binary operation on $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ is never a group with respect to multiplication.

0 does not have inverse, because $0 \cdot x = 0$

Even if we remove 0, there are still some complications.

Example: $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

$2 \cdot 0 = 0$ $\quad$ $2 \cdot 2 = 0$

$2 \cdot 1 = 2$ $\quad$ $2 \cdot 3 = 2$

So 2 does not have an inverse.

Observation: Suppose $a \neq 0 \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse. Then there exists some $x \in \mathbb{Z}/m\mathbb{Z}$ such that

$$ax \equiv 1 \pmod{m}$$

$$\iff ax - 1 = my \text{ for some } y \in \mathbb{Z}$$

$$\iff ax - my = 1$$

$$\iff \gcd(a, m) = 1$$

We will prove below why these two statements are equivalent.

Definition (GCD) Let a and b be two integers. We say that d is the gcd of a and b if

i) $d > 0$

ii) If $c \mid a$ & $c \mid b$, then $c \mid d$.

How do you Compute GCD

(1) Method 1 (From prime factorization)

$$a = p_1^{q_1} \cdots p_r^{q_r}$$

$$b = p_1^{b_1} \cdots p_r^{b_r}$$

$$\gcd(a,b) = p_1^{\min(q_1,b_1)} \cdots p_r^{\min(q_r,b_r)}$$

(2) Method 2 (Writing gcd as a linear combination of two elements)

Say $b < a$

$$a = bq_0 + r_0$$

$$b = r_0 q_1 + r_1 \quad 0 \le r_1 < r_0 < b$$

$$\vdots$$

$$r_i = r_{i+1} q_{i+2} + r_{i+2}$$

$$\vdots$$

This will terminate

$$r_j = r_{j+1} q_{j+2}$$

r_{j+1} is the GCD

Example: Find GCD of 13 & 21.

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1 \longrightarrow$ GCD

$2 = 1(2) + 0$

Tracing back, we can write 1 as a linear combination of 21 & 13.

$1 = 3 - 2$

$1 = 3 - [5-3] = 3 - 5 + 3 = 3(2) - 5$

$1 = 8(2) - 5(2) - 5$

$= 8(2) - 5(3)$

$1 = 8(2) - (13-8)(3) = 8(5) - 13(3)$

$1 = 21(5) - 13(8)$

Generally, we can write $\gcd(a,b)$ as a linear Combination of a and b.

Lemma: Let a & b be two integers. Then there exist $x, y \in \mathbb{Z}$ s.t $ax+by=1 \iff \gcd(a,b)=1$.

Pf: $\Rightarrow$ Suppose $ax+by=1$

If $c \mid a$ & $c \mid b \Rightarrow c \mid 1 \Rightarrow c$ is the gcd.

$\Leftarrow$: As discussed above

The above lemma is not true if $\gcd(a,b)>1$

Example: $8(1)-2(2)=4$

but 4 is not gcd of 8 and 2.

Here is a refined version of above lemma.

Lemma: If d is the Smallest positive integer s.t $d=ax+by$ for some $x, y \in \mathbb{Z}$, then $d=\gcd(a,b)$.

Pf: Exercise (HW 3)

$\mathbb{Z}/m\mathbb{Z}$

$a \in \mathbb{Z}/m\mathbb{Z}$ has a multiplicative inverse $\iff \gcd(a, m) = 1$

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{ a \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1 \}$$

Examples: $m = 9$

$$(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$$

$m = 10$

$$(\mathbb{Z}/10\mathbb{Z})^\times = \{1, 3, 7, 9\}$$

$(\mathbb{Z}/m\mathbb{Z})^\times$ is a group with respect to multiplication.

Chinese Remainder Theorem

Suppose $m = p_1^{q_1} p_2^{q_2} p_3^{q_3} \cdots p_r^{q_r}$

Define $f: \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \longrightarrow \left(\mathbb{Z}/p_1^{q_1}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{q_r}\right)^\times$

$$a \longmapsto \left(a \pmod{p_1^{q_1}}, \cdots, a \pmod{p_r^{q_r}}\right)$$

We can think of $\left(\mathbb{Z}/p_1^{q_1}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{q_r}\right)^\times$ as a group.

$$(m_1, m_2, \cdots, m_r)(n_1, n_2, \cdots, n_r) = (m_1 n_1, \cdots, m_r n_r)$$

(CRT) f is a group isomorphism.

Pf: (1) We need to show that f is a group homomorphism.

$$f(ab) = \left(ab \pmod{p_1^{q_1}}, \ldots, ab \pmod{p_r^{q_r}}\right)$$

$$= \left(a \pmod{p_1^{q_1}}, \ldots, a \pmod{p_r^{q_r}}\right)$$

$$\left(b \pmod{p_1^{q_1}}, \ldots, b \pmod{p_r^{q_r}}\right)$$

$$= f(a)\, f(b)$$

(2) $\ker f = \{ a \mid a \equiv 1 \pmod{p_i^{q_i}} \ \forall i \}$

$$= \{ a \mid a \equiv 1 \pmod{m} \}$$

$$= \{ 1 \}$$

(3) Pick $(x_1, \ldots, x_r)$ in co-domain

We will construct an $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ s.t

$$f(a) = (x_1, \ldots, x_r)$$

$\prod_{j \neq i} p_j^{q_j}$ is coprime to $p_i^{q_i}$

Suppose y_i satisfies $y_i \prod_{j \neq i} p_j^{q_j} \equiv 1 \pmod{p_i^{q_i}}$

Take $a = x_1 y_1 p_2^{q_2} \cdots p_r^{q_r}$

$$+ x_2 y_2 p_1^{q_1} p_3^{q_3} \cdots p_r^{q_r}$$

$$\vdots$$

$$+ x_r y_r p_1^{q_1} p_2^{q_2} \cdots p_{r-1}^{q_{r-1}}$$

$$a \pmod{p_1^{q_1}} = x_1$$

$$a \pmod{p_2^{q_2}} = x_2$$

$$\vdots$$

$$a \pmod{p_r^{q_r}} = x_r$$

So, f is an isomorphism.

Therefore size of $(\mathbb{Z}/m\mathbb{Z})^\times$ is equal to size of $(\mathbb{Z}/p_1^{q_1})^\times \times \cdots \times (\mathbb{Z}/p_r^{q_r})^\times$

Qn: 1) Is $(\mathbb{Z}/m)^\times$ abelian ?

2) Is it cyclic ?

Size of $(\mathbb{Z}/m\mathbb{Z})^\times$

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{ 1 \le a \le m-1 \mid \gcd(a, m) = 1 \}$$

Euler's totient function (or Euler's phi function)

$$\phi(m) = \{ 1 \le a \le m-1 \mid \gcd(a, m) = 1 \}$$

Case 1: If m is prime

$$\phi(p) = p - 1$$

Case 2: If $m = p^a$, p prime

1	2	3	. . . .	$p-1$	p
$p+1$	$p+2$		. . . .	$2p-1$	$2p$
:				:	:
$p^a-(p-1)$		- -		p^a-1	p^a

1	2	3	$p-1$	p
$p+1$	$p+2$		$2p-1$	$2p$
⋮			⋮	⋮
$p^a-(p-1)$			p^a-1	p^a

Only Multiples of p

$$\phi(m) = p^a - p^{a-1}$$

Lemma: If $\gcd(m,n) = 1$, then

$$\phi(mn) = \phi(m)\,\phi(n)$$

Pf: Chinese remainder theorem

If $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$

$$\phi(m) = \phi(p_1^{a_1}) \cdots \phi(p_r^{a_r})$$

$$= p_1^{a_1-1}(p_1-1) \cdots p_r^{a_r-1}(p_r-1)$$

Looking at Construction of $\mathbb{Z}/m\mathbb{Z}$ again

Summary: We defined an equivalence relation on $\mathbb{Z}$ & $\mathbb{Z}/m\mathbb{Z}$ is just a set of those equivalence classes.

Goal: Let us try to generalize this Construction in terms of subgroups.

$(\mathbb{Z}, +)$ is a group.

Qn: What are all the subgroups of $(\mathbb{Z}, +)$?

Ans: $\{0\}$, $\mathbb{Z}$ are obvious ones.

Suppose H is a subgroup of $\mathbb{Z}$ that is not $\{0\}$ or $\mathbb{Z}$.

Here are some observations about H

i) $1 \notin H$ because then $H = \mathbb{Z}$.

ii) H contains both positive and negative integers.

Suppose m is the smallest positive integer that lies in H.

Then $H = \{\ldots, -2m, -m, 0, m, 2m, 3m, \ldots\}$

because if $b > 0 \in H$ & b is not a multiple of m then

$$b = mq + r \quad 0 < r < m$$

$$r = \underbrace{b - mq}_{\in H}$$

which is contradiction

Let's denote $H = \{\ldots, -m, 0, m, 2m, \ldots\}$ as $m\mathbb{Z}$.

So, all the subgroups of $\mathbb{Z}$ are of the form $m\mathbb{Z}$.

Equivalence Relation	Restating that in terms of subgroups
$a \sim b \iff a$ & b leave the same remainder when divided by m $\iff a-b$ is a multiple of m	$a \sim b \iff a-b \in m\mathbb{Z}$ in general G group H subgroup of G $a \sim b \iff ab^{-1} \in H$

Let's explore this!

G group $\quad H \leq G$ Subgroup

Define a relation on G as follows:

$$a \sim b \iff ab^{-1} \in H$$

Equivalence classes are called <u>Cosets</u>.

$$G/H = \{ \text{Set of cosets} \}$$

$ab^{-1} \in H$, $ab^{-1} = h$ for some $h \in H$

$$a = hb$$

$$a \in Hb$$

$$G/H = \{ Hb \mid b \in G \}$$

Some questions to ponder:

1. Is G/H a group?
2. Is G/H always finite?

(Will discuss next time)